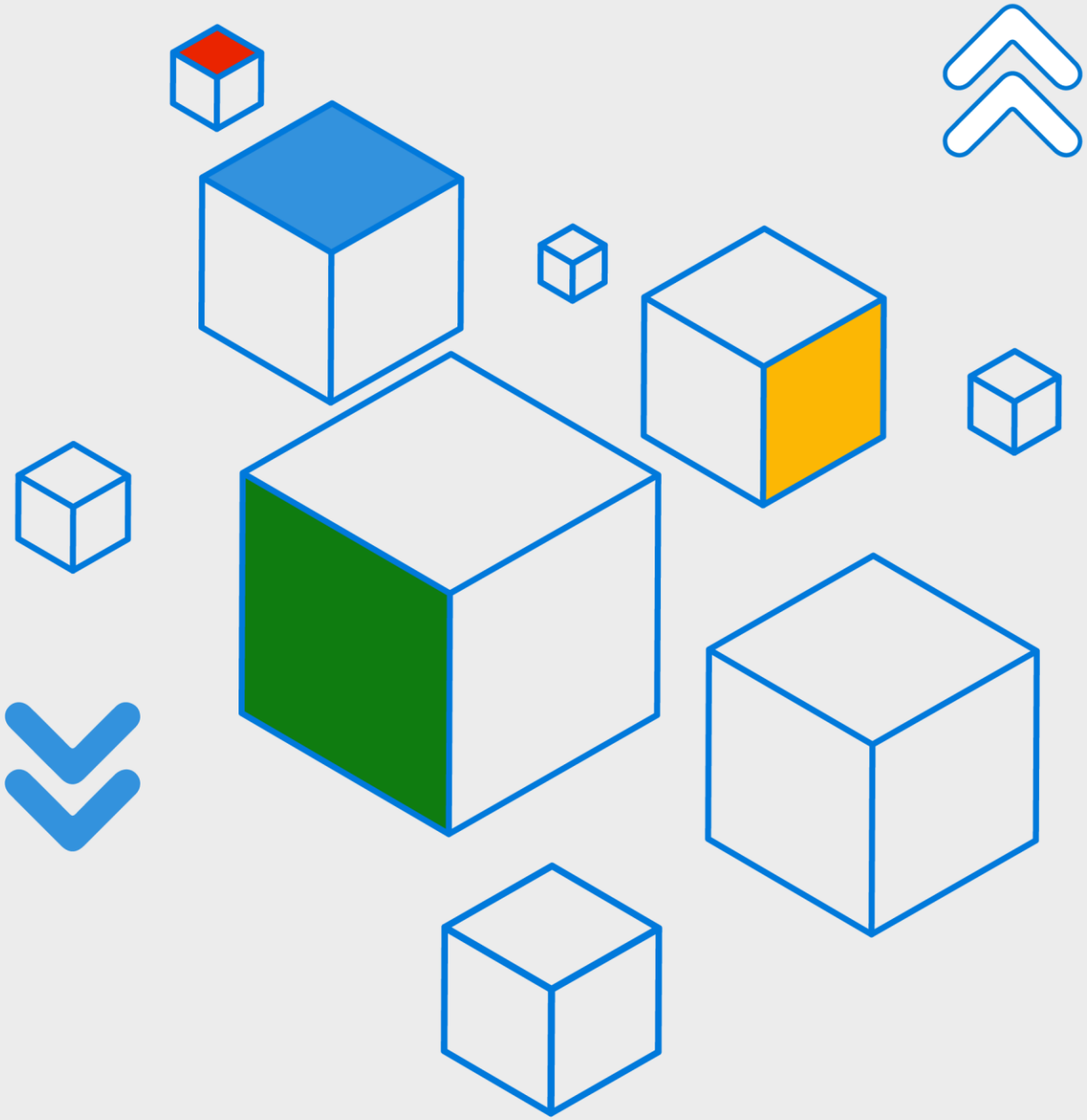
Deep Dive:

Single Sign-On for Azure Virtual Desktop and Windows 365



Grace Picking

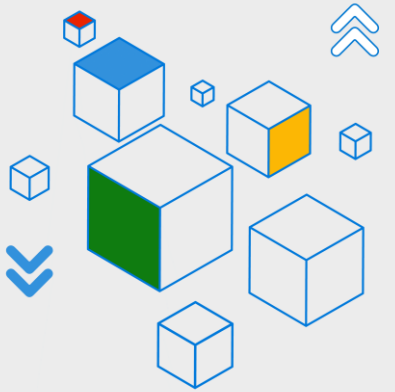
Sandeep Deo

David Belanger

425Show

425Show

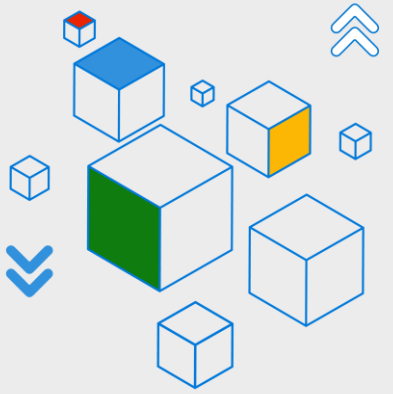
AGENDA



- What
- Why
- How
- Pre-requisites
- Authentication flow
- Demo
- Roadmap
- Q&A

425Show

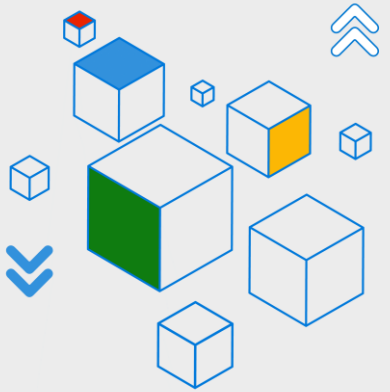
Single Sign-On - What



- Enable the most secure and productive Azure native, OS and credential agnostic Remote Desktop (RD) connection experience with Entra ID for Azure Virtual Desktop (AVD) and Windows 365 (W365) deployments.
- Support passwordless authentication on all platforms.
- Enforce security using Conditional Access like any other application.
- Provide Single Sign-On inside the session for Entra ID based apps and websites.
- No complex infrastructure required and just works with Entra ID.
- Works with existing services and no need for additional infrastructure.
- Generally available since Microsoft Ignite in November 2023.

425Show

Single Sign-On - Why



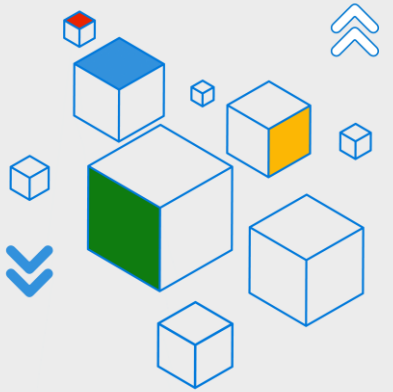
- Previous authentication capabilities for Remote Desktop experience:
  - Offered limited platform and passwordless credential support (e.g. smartcard/Windows Hello For Business on Windows native client, password only on other platforms)
  - Required Windows client device to have a device identity with Entra ID.
  - Did not offer Single Sign-On (SSO) support.

- Provide support for other IdP that federate with Entra ID.

- Mandated by Executive Order 14028 that government agencies must move to adopt phishing-resistant multi-factor authentication (MFA) that includes RD connection experience.

425Show

Single Sign-On - How



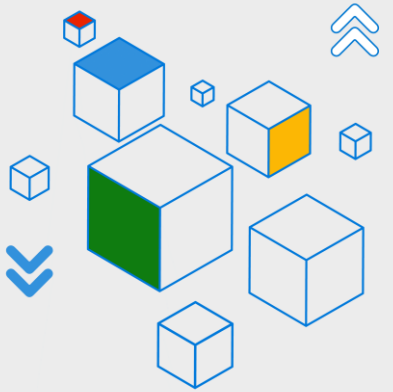
- Entra ID added support for:
  - A new protocol using RDP access token for approved apps.
  - An admin configurable Service Principal policy for SSO.
  - An admin configurable Conditional Access policy for strong authentication.

- RD team added support for:
  - All AVD/W365 clients and Remote Desktop Connection client (MSTSC) to use RDP access token to authenticate to the session host.
  - Configurable AVD host pool RDP Property and W365 Provisioning Policy to enable SSO.
  - MSTSC UI updated to expose the new authentication method.

- Windows team added support for:
  - RDP Credential provider to handle RDP access token.
  - Signing in user with RDP access token.

425Show

Single Sign-On – Pre-requisites



- AVD session host/W365 PC:
  - OS: Windows 10/11, Windows Server 22 with Oct 2022 update
  - Join state: Entra joined or Entra hybrid joined. Not supported with domain joined
  - Create a Kerberos Server Object for Entra hybrid joined

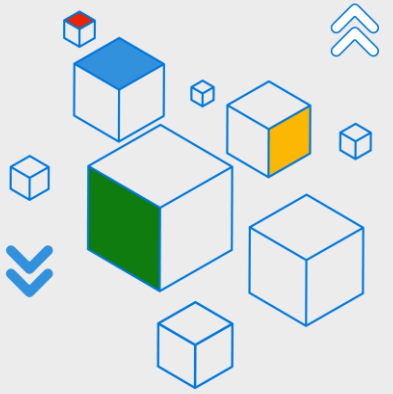
- Local device:
  - Platforms: Windows (10/11), Web, macOS, iOS, Android
  - Join state: No requirement

- User:
  - Cloud native or hybrid

- Identity Provider:
  - Microsoft Entra ID
  - Third-party IDP integrated with Microsoft Entra ID

425Show

Single Sign-On – Auth flow

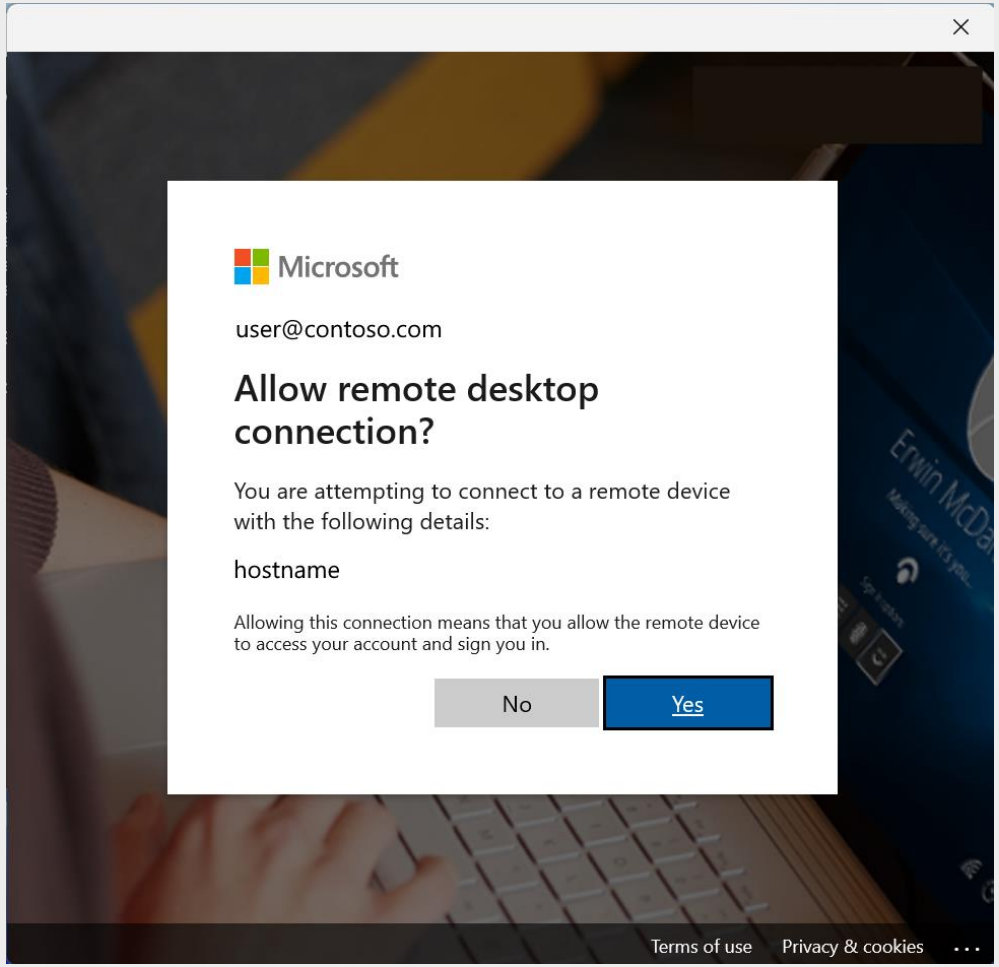


1. Client requests an RDP access-token for the target host (DeviceID \FQDN in Entra).
2. Entra ID issues an RDP access-token (bound to the client and target device) to the client after:
   - user authenticates and accepts the consent prompt for the host, unless the host has been consented to by the user previously or via SSO policy configured by the admin.
   - all applicable Conditional Access policies are satisfied.
3. Client now connects to the target host with TLS Handshake and sends the RDP access-token for the credential.
4. Target host receives the RDP access-token, validates it, and then does the Network Logon to authenticate the user.
5. At this stage, the RDP access-token is consumed by the target logon stack to authenticate to Entra ID and a remote logon session is spawned.
   - Entra ID issues a PRT (Primary Refresh Token) and a Kerberos TGT.
   - User can now access cloud and on-prem resources alike, eg: access Azure Files.
6. RDP also handles session reconnects as usual by going back to Step 1, if needed.

425Show

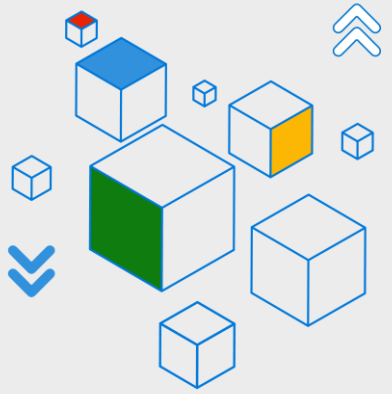
Single Sign-On – Consent Prompt

- Enabled by default
- Replaces untrusted cert warning
- Save the last 15 hosts for 30 days
- Admin can configure SSO policy to pre-consent target machines using device groups



425Show

Single Sign-On – Conditional access policies

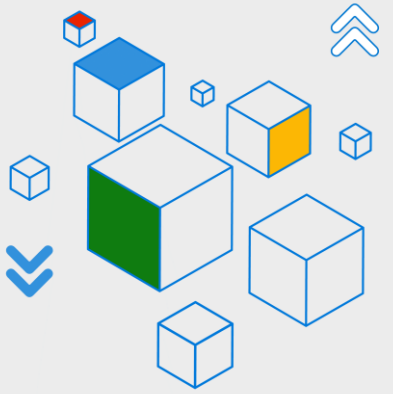


Connecting To	AVD RDWeb (Subscription)	AVD RD Gateway	AVD Session Host
Client ID	Azure Virtual Desktop Client	Azure Virtual Desktop Client	Azure Virtual Desktop Client
Resource ID	Azure Virtual Desktop	Azure Virtual Desktop	Microsoft Remote Desktop (today) Windows Cloud Login (soon)

- Azure Virtual Desktop (CA enabled)
  - 9cdead84-a844-4324-93f2-b2e6bb768d07
- Microsoft Remote Desktop (CA enabled)
  - a4a365df-50f1-4397-bc59-1a1564b8bb9c
- Windows Cloud Login (CA enabled)
  - 270efc09-cd0d-444b-a71f-39af4910ec45

425Show

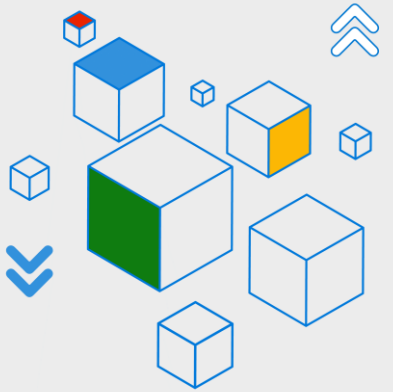
Single Sign-On – Session lock behavior



- New behavior when the session locks from a policy or user interaction.
- Session disconnects instead of showing the remote lock screen.
- Reasons for this change:
  - Remote lock screen is not considered a security boundary.
  - Remote lock screen doesn't support passwordless credentials like FIDO and some WHfB configurations.
  - Ensures Conditional Access policies are re-evaluated.
  - Provides consistent authentication, always through Entra ID.
- Option to make this behavior configurable expected to be available in 2024.

425Show

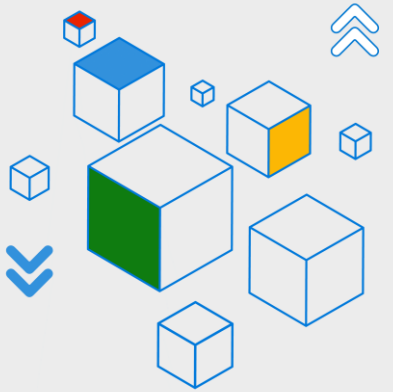
In-session passwordless - What



- Provide support for Windows Hello for Business, FIDO keys and future auth methods inside the session.
- Doesn’t expose the local biometrics and security devices to the host.
- Support nested sessions.

425Show

In-session passwordless - How

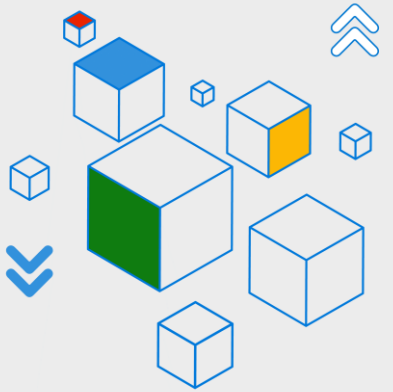


- Windows webauthn.dll enhanced to exposed an RDP plugin.
- Plugin automatically loaded by the RD client and remotely by the terminal service component (TermServ).
- New RDP property to enable/disable the redirection.
- Also controlled using Group Policy and Intune Policy.

aka.ms/425show/AVDInSessionAuth

425Show

In-session passwordless – Pre-requisites



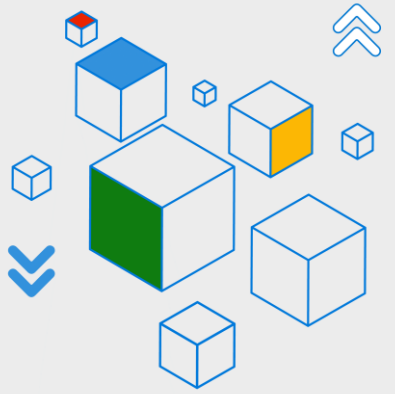
- AVD session host/W365 PC:
  - OS: Windows 10/11, Windows Server 22 with Oct 2022 update

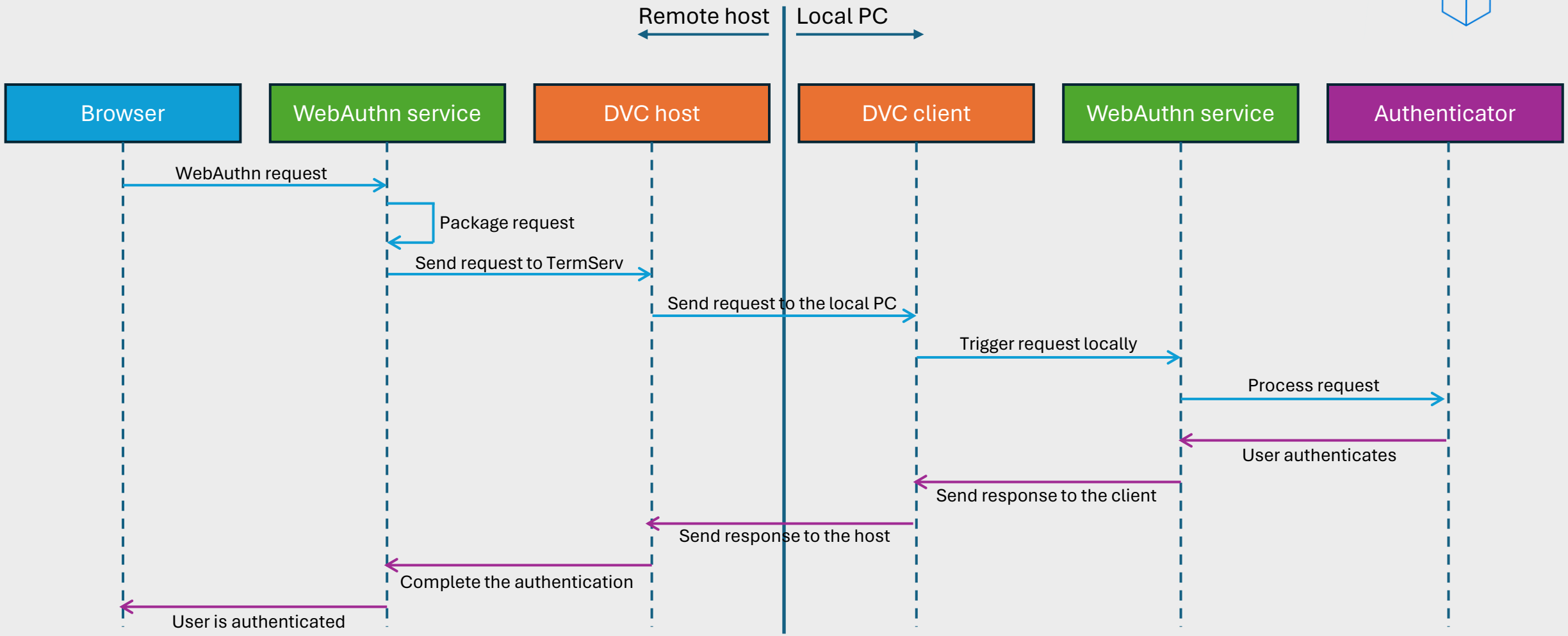
- Local device:
  - Windows 10/11, Windows Server 22 with Oct 2022 update
  - Windows only support for now

- FIDO configuration for Microsoft Entra ID apps and sites:
  - User added to the FIDO2 Security Key Authentication Methods policy
  - FIDO device registered in Microsoft Entra ID (Required for Second factor proof up)

425Show

In session passwordless with WebAuthn redirection – Auth flow





425Show

Demo

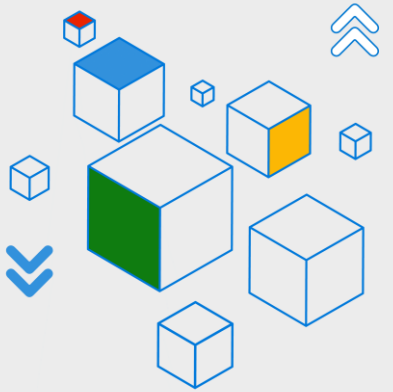
- AVD single sign-on for Windows
- AVD WebAuthn Redirection
- Remote Desktop Security Configuration on Service Principal for enabling SSO

425Show

Roadmap

- Microsoft Entra ID re-authentication after 15 minutes when connecting to AVD and W365.
- Entra ID support for FIDO security keys on macOS, iOS and Android.
- B2B user logon support for AVD and W365.
- Certificate based auth for Linux clients when connecting to AVD and W365.
- Admin UX for configuration SSO policy (remoteDesktopSecurityConfiguration) on Service Principal.

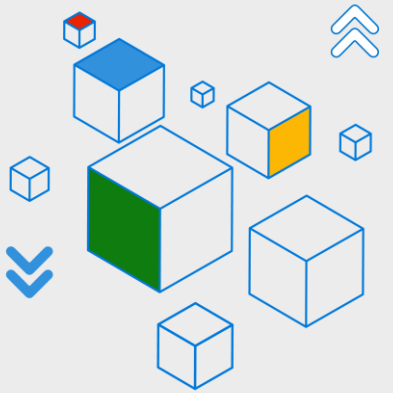
425Show



Q&A

425Show

Resources



- **Documentation for SSO with Azure Virtual Desktop and Entra ID**
  - aka.ms/425show/AVDSSO
- **Documentation for in-session passwordless**
  - aka.ms/425show/AVDInSessionAuth
- **Identities and authentication for Azure Virtual Desktop**
  - aka.ms/425show/AVDIdentities

Thank you for tuning in!

Don’t forget to tune in for future shows!

425Show